The Autocorrelation Theoretic Estimation of non-Linear Key Generator Sequences

Prof. Dr. Abdul Monem S. Rahma
University of Technology

Ayad G. Nasser
University of Technology

Abstract :

The Randomness is one of the basic criterions to measure Key Generator Efficiency. The key generator depends basically on Linear FeedBack Shift Register which is considered as one of the basic units of Stream Cipher Systems. In this paper, the autocorrelation postulate, which one of the basis of Randomness criteria, is calculated theoretically for non-linear key generator before it be implemented or constructed (software or hardware), this procedure save time and costs. Two non-linear key generators are chosen to apply the theoretical studies, these key generators are the Product and Brüer.

1. Introduction

Linear Feedback Shift Register (LFSR) and Combining Function (CF) are considered as basic units to construct key generator (KG) that used in stream cipher systems [1]. Any weakness in any one of these units means clear weakness in KG sequence, so there are some conditions must be available in KG before it is constructed; therefore the KG efficiency is concluded.

In this paper, some studies are applied on the KG sequences to determine the sequence autocorrelation. The Basic efficiency for KG can be defined as the ability of KG and its sequence to withstand the mathematical analytic which the cryptanalyst applied on them, this ability measured by some basic criterions, the most important is the randomness, one of the randomness postulates is the autocorrelation postulate.

In the next part of this paper, the autocorrelation postulate of randomness criterion will be discussed in details and introduce the basic conditions to obtain efficient KG specially those related to autocorrelation. It's important to mention that the zero input sequences must be avoided, this done when the non-all zeros initial values for LFSR's are chosen.

Let KG consist of n-LFSR's have lengths $r_1,r_2,..,r_n$ respectively with $CF=F_n(x_1,x_2,\ldots,x_n)$, s.t. $x_i \in \{0,1\}$ $1 \le i \le n$, represents the output of $LFSR_i$, let $S=\{s_0,s_1,\ldots\}$ be the sequence product from KG and s_j, $j=0,1,\ldots$ represents elements of S. let S_i be the sequence i product from $LFSR_i$ with a_{ij} elements $1 \le i \le n$, $j=0,1,\ldots,$. Two cases study are chosen, the product KG using the non-linear product CF s.t $F_n(x_1,x_2,..,x_n)=\prod_{i=1}^{n} x_i$, and the Brüer KG [2] using the non-linear CF s.t $F_n(x_1,x_2,x_3)=x_1x_2 \oplus x_1x_3 \oplus x_2x_3$.

2. Conditions of the Theoretical Estimation

Definition (1) [3]: Let $GCD_2=gcd(\prod_{i=1}^{1} m_i, m_2.GCD_1)=gcd(m_1,m_2)$, for convenient let $GCD_1=1$ and so on the general form of the recursion equation will be:

$$GCD_n=gcd(\prod_{i=1}^{n-1} m_i, mn.GCD_{n-1}) \quad \ldots(1)$$

where n≥2 s.t mi are positive integers, ∀1≤i≤n.

Let the sequence S has period P(S), the period of $LFSR_i$ denotes by $P(S_i)$, P(S) and $P(S_i)$ are least possible positive integers, so

$P(S)=lcm(P(S_1),P(S_2),\ldots,P(S_n))$

$$P(S)=\frac{\prod_{i=1}^{n} P(S_i)}{GCD_n(P(S_i))} \qquad \ldots(2)$$

$$\text{s.t. } GCD_n(P(S_i))=\gcd\left[\prod_{i=1}^{n-1} P(S_i), P(S_n)\cdot GCD_{n-1}(P(S_i))\right] \qquad \ldots(3)$$

If $P(S_i)$ are relatively prime with each other this mean $GCD_n(P(S_i))=1$ this implies [3]:

$$P(S)=\prod_{i=1}^{n} P(S_i) \qquad \ldots(4)$$

It's known earlier that $P(S_i) \le 2^{r_i}-1$, and if the $LFSR_i$ has maximum period then $P(S_i)= 2^{r_i}-1$ [4].

<u>Theorem (1)</u> [3]

$P(S)=\prod_{i=1}^{n}(2^{r_i}-1)$ if and only if the following conditions are holds:

1. **$GCD_n(P(S_i))=1$,.**
2. **the period of each LFSR has maximum period ($P(S_i)=2^{r_i}-1$).**

3. Randomness

The sequence that is satisfied the 3-randomness properties called Pseudo Random Sequence (PRS) [4]. The randomness criterion depends on LFSR's and CF units, therefore from the important conditions to get PRS is, the sequence must be maximal and CF must be balance [5].

To guarantee the KG to produces PRS, the sequence must pass randomness tests with complete period, these tests applied into two ways, on: [1]

1. **Global sequence for complete period and that is the right way (but it's hard to applied for high periods).**
2. **Local sequence for many times for various lengths less than the origin length.**

In this part, the 1st way will be applied theoretically for any period.

If $GCD_n(P(S_i))=1$ then,

$$P(S)=2^{\sum_{i=1}^{n} r_i}+(-1)\cdot(2^{r_1+\cdots+r_{n-1}}+\cdots+2^{r_2+\cdots+r_n}+\cdots+(-1)^{n-1}\cdot(2^{r_1}+\cdots+2^{r_n})+(-1)^n \quad \text{...(5)}$$

Let R_m^t denotes the combination to sum m of numbers r_i from n of the numbers r_i, R_m denotes the set of all possibilities of R_m^t s.t.

$$R_m^t=\begin{pmatrix} r_1, r_2, \ldots, r_n \\ \sum_{j=1}^{m} r_{i_j} \end{pmatrix} \quad 0\le m\le n,\ 1\le i\le n,\ t\in\{1,2,\ldots,C_m^n\}$$

define $R_0=\{R_0^1\}$, $R_0^1=0$.

For instance let m=1 then $R_1=\{R_1^1,R_1^2,\ldots,R_1^{C_1^n}\}, R_1^1=r_1,\ldots,R_1^n=r_n$

If m=n then $R_n=\{R_n^1\}$, $R_n^1=\sum_{i=1}^{n} r_i$

So equation (5) can be written in compact formula:

$$P(S)=\sum_{k=0}^{n}(-1)^k\cdot\sum_{t=1}^{C_k^n}2^{R_{n-k}^t} \quad \text{...(6)}$$

Golomb deduced three theorems about the Maximal Sequence (MS) generated from LFSR [4]. One of the three Golomb's theorems deduced from the autocorrelation postulate.

In the next sections we will introduce new theorems, as Golomb do on LFSR, to prove the good autocorrelation distribution of Brüer KG and the weak randomness of the product KG by applying the autocorrelation postulates.

4. Autocorrelation Postulate

Before we involve in details of calculating this part of randomness criterion we have to give some preliminaries.

Let $S_r=\{a_j\}_{j=0}^{p(S_r)-1}$ be the sequence generated from maximum LFSR, s.t. $a_j \in \{0,1\}$. In corresponding let $Q_r=\{b_j\}_{j=0}^{p(S_r)-1}$ denotes the transform sequence gotten from the following linear transform:

$b=1-2a$ ...(7)

Where $b_j \in \{-1,1\}$.

a=0,1, then is corresponding b=1, -1 respectively.

Definition (2): When the LFSR has maximum period s.t. $P(S_r)=2^r-1$, then its can generates k sequences A_k, $1 \le k \le P(S_r)-1$, each generated using the initial vector v_k s.t. $A_k=\{a_{k_j}\}_{j=0}^{p(S_r)-1}$, ($A_0=\{0,0,\ldots,0\}$), then the set $A=\{A_0,A_1,\ldots,A_{P(Sr)-1}\}$ with XOR $\oplus$ operation $\langle A,\oplus\rangle$ form a group [4].

Golomb mentioned that for MS the $\sum_{i=0}^{P(S_r)-1} a_i = 1$ and $\sum_{i=0}^{P(S_r)-1} b_i = -1$, and $P(S_r)=P(Q_r)=N_Q(1)+N_Q(-1)$.

<u>Definition (3):</u> Let $B_k=\{b_{k_j}\}_{j=0}^{P(S_r)-1}$ be the corresponding to A_k mentioned above when $0 \le k \le P(S_r)-1$, ($B_0=\{1,1,\ldots,1\}$), then they form a set $B=\{B_0,B_1,\ldots,B_{P(Sr)-1}\}$.

<u>Lemma (1) [4]:</u>

Let $B=\{B_0,B_1,\ldots,B_{P(r)-1}\}$ be a non-empty set as defined above, then $\langle B,\cdot\rangle$ is a group.

As known:

$a_1+a_2=a_1 \oplus a_2 \oplus a_1a_2$ **…(8)**

and

$a_1 \oplus a_2=a_1+a_2-2a_1a_2$ **…(9)**

The generalization of equation (9) given in the next lemma.

Lemma (2):

Let $a_i \in \{0,1\}$, $1 \le i \le n$ then:

$$\sum_{i=1}^{n}{}^{\oplus} a_i = \sum_{i=1}^{n} a_i - 2(a_1a_2+\ldots+a_{n-1}a_n)+\ldots+(-1)^{n-1}.2^{n-1}.\prod_{i=1}^{n} a_i \quad \text{…(10)}$$

Proof:

Equation (10) is true from equation (9).

Let's assume that equation (10) is true, we have to prove that its true for n+1.

$$\sum_{i=1}^{n} a_i \oplus a_{n+1} = \sum_{i=1}^{n} - 2(a_1a_2+\ldots+a_{n-1}a_n)+\ldots+(-1)^{n-1}.2^{n-1}.\prod_{i=1}^{n} a_i$$

$$+ a_{n+1} - 2(\sum_{i=1}^{n} a_i + \ldots + (-1)^{n-1}.2^{n-1}\prod_{i=1}^{n} a_i)a_{n+1} \quad \text{…(11)}$$

After simplify equation (11) we get:

$$\sum_{i=1}^{n+1}{}^{\oplus} a_i = \sum_{i=1}^{n+1} a_i - 2(a_1a_2+\ldots+a_na_{n+1})+\ldots+(-1)^{n}.2^{n}.\prod_{i=1}^{n+1} a_i$$

$\therefore$ equation (10) is true for n+1, that implies its true $\forall$n.

Definition (4): Lets $C_r(\tau)$ be the auto correlation function of maximal sequence which is generated from LFSR with length r and shifted by integer τ s.t [4]:

$C_r(\tau) = \frac{1}{P(S_r)} d_r(\tau)$, **where**

$$d_r(\tau) = \sum_{k=0}^{P(S_r)-1} b_k b_{k+\tau} = \begin{cases} P(S) & \tau = 0, P(S_r) \\ -1 & 0 < \tau < P(S_r) \end{cases} \quad \text{...(12)}$$

Remark (1): **$d_r(\tau)$ can represents the difference between $N_r(1)$ and $N_r(-1)$ of the sequence Q_r after shifted by τ.**

Definition (5): **The auto correlation function $C_S(\tau)$ of the sequence S (or the corresponding sequence Q) which is generated from system of LFSR's can be defined as follows:**

$$\left.\begin{aligned} C_S(\tau) &= \frac{1}{P(S)} d_S(\tau), \text{ where} \\ d_S(\tau) &= \sum_{k=0}^{P(S)-1} q_k q_{k+\tau} \end{aligned}\right\} \quad \text{...(13)}$$

Where $q_k \in \{-1,1\}$ is the element k of the sequence Q.

Remark (2): **$d_S(\tau)$ represents the difference between $N_S(1)$ and $N_S(-1)$ of the sequence Q after shifted τ.**

Definition (6): **Let T_k^t denotes the combination to multiply k of $P(S_i)$ from the total number n of $P(S_i)$, $1 \le i \le n$.**

Let T_k denotes the set of all possibilities of T_k^t, s.t.

$$T_k^t = \left(\prod_{i=1}^{k} P(S_{i_j}) \right)_{P(S_1),\ldots P(S_n)}$$ **, $0 \le k \le n$, $t \in \{1,2,\ldots, C_k^n\}$,**

we defined $T_0 = \{T_0^1\}$, $T_0^1 = 1$

For instance, let k=1, then $T_1 = \{T_1^1, T_1^2, \ldots, T_1^n\}$, $T_1^i = P(S_i)$, $1 \le i \le n$.

When k=n, then $T_1=\{T_n^1\}$, s.t. $T_n^1 = \prod_{j=1}^{n} P(S_j)$

Definition (7): **Let the CF be F_n, s.t. F_n:A→{0,1}, let H_n be the corresponding function of F_n s.t. H_n:B→{-1,1}.**

Lemma (3):

If F_n is the linear function s.t. $s=F_n(a_1,a_2,\ldots,a_n)=\sum_{i=1}^{n}{}^{\oplus} a_i$, then $q=H_n(b_1,b_2,\ldots,b_n)=\prod_{i=1}^{n} b_i$

Where s and q are the output element of the functions F_n and H_n respectively.

Proof: **By using equation (7):**

$$s=\frac{1}{2}(1-q) \qquad \ldots(14)$$

From equation (11) and lemma (2)

$$s=F_n(a_1,a_2,\ldots,a_n)=\sum_{i=1}^{n}{}^{\oplus} a_i = \sum_{i=1}^{n} a_i - 2(a_1a_2+\ldots+a_{n-1}a_n)+\ldots+(-1)^{n-1}.2^{n-1}.\prod_{i=1}^{n} a_i$$

Reuse equation (7) in a_i and b_i we get:

$$s=\tfrac{1}{2}\sum_{i=1}^{n}(1-b_i)-2[(1-b_1)+\cdots+(1-b_n)]+\ldots+(-1)^{n-1}.2^{n-1}.\frac{1}{2}.\prod_{i=1}^{n}(1-b_i) \qquad \ldots(15)$$

When simplify equation (15) we get:

$$s=\frac{1}{2}\left(1-\prod_{i=1}^{n} b_i\right) \qquad \ldots(16)$$

Compare equation (16) with (14) we get:

$$q=H_n(b_1,b_2,\ldots,b_n)=\prod_{i=1}^{n} b_i$$

The next lemma discusses the behavior of H_n when F_n is the product function.

Lemma (4): If F_n is the product function s.t.

$s = F_n(a_1,a_2,\ldots,a_n) = \prod_{i=1}^{n} a_i$, then:

$$q = H_n(b_1,b_2,\ldots,b_n) = \Delta_{i=1}^{n} b_i = 1 - \frac{1}{2^{n-1}} \prod_{i=1}^{n} (1-b_i) \quad \ldots(17)$$

Where Δ (read delta) represents the multiple of (×) operation (it can be denoted by *).

Proof:

$$s = \prod_{i=1}^{n} a_i = \prod_{i=1}^{n} \frac{1}{2}(1-b_i) = \frac{1}{2^n} \prod_{i=1}^{n} (1-b_i)$$

Since $s = \frac{1}{2}(1-q)$, then $q=1-2s$

$$\therefore 2s = \frac{1}{2^{n-1}} \prod_{i=1}^{n} (1-b_i)$$

$$\therefore q = \Delta_{i=1}^{n} b_i = 1 - \frac{1}{2^{n-1}} \prod_{i=1}^{n} (1-b_i)$$

Of course, if $GCD_n(P(S_i))=1$, then:

$q_m = H_n(b_{1m},b_{2m},\ldots,b_{nm})$, m=0,1,…,P(S)-1.

Product System (n-PKG)

Golomb mentioned that if the algebraic system ({0,1},⊕,•) form a filed, then algebraic system ({-1,1},×,*) is a filed too [4], s.t. 1 and -1 are identity elements of the operations × and * respectively, s.t.

*	1	-1
1	1	1
-1	1	-1

As mentioned before, we construct the symbol Δ to denote the relation * by (see equation (17)):

$$\bigtriangleup_{i=1}^{n} b_i = 1 - \frac{1}{2^{n-1}} \prod_{i=1}^{n} (1 - b_i) \quad \text{...(18)}$$

Lemma (5):

$$\sum_{m=0}^{P(S)-1} q_m = \prod_{i=1}^{n} P(S_i) - \frac{1}{2^{n-1}} \prod_{i=1}^{n} 2^{r_i} = \prod_{i=1}^{n} P(S_i) - 2^{\sum_{i=1}^{n} r_i - n + 1} \quad \text{...(19)}$$

Proof:

Since $\{b_{im}\}$ are maximal sequences with period $P(S_i)$, then:

$$\sum_{m=0}^{P(S)-1} q_m = \sum_{j_1=0}^{P(S_1)-1} \cdots \sum_{j_n=0}^{P(S_n)-1} \left[1 - \frac{1}{2^{n-1}} \prod_{i=1}^{n} (1 - b_{ij_i}) \right] = \prod_{i=1}^{n} P(S_i) - \frac{1}{2^{n-1}} \prod_{i=1}^{n} \left[(2^{r_i} - 1) - \sum_{j_i=0}^{P(S_i)-1} b_{ij_i} \right]$$

As mentioned before $\sum_{j=1}^{P(S)} b_i = -1$, then the above equation will be:

$$\sum_{m=0}^{P(S)-1} q_m = \prod_{i=1}^{n} P(S_i) - \frac{1}{2^{n-1}} \prod_{i=1}^{n} 2^{r_i} = \prod_{i=1}^{n} P(S_i) - 2^{\sum_{i=1}^{n} r_i - n + 1}$$

Now we will shifting Q by $0<\tau\le P(S)-1$ to find $d_S(\tau)$ by using the next theorem.

Theorem (2):

$$d_S(\tau) = \prod_{i=1}^{n} P(S_i) - 2^{\sum_{i=1}^{n} r_i - n + 2} + \frac{1}{2^{2n-2}} \prod_{i=1}^{n} \left[2^{r_i} + 1 + d_{r_i}(\tau_i) \right] \quad \text{...(20)}$$

Proof:

Since $\{b_{im}\}$ are maximal sequences with period $P(S_i)$, then:

$$d_S(\tau) = \sum_{m=0}^{P(S)-1} S_m S_{m+\tau} = \sum_{m=0}^{P(S)-1} \bigtriangleup_{i=1}^{n} b_{im} \bigtriangleup_{i=1}^{n} b_{i,m+\tau} = \sum_{j_1=0}^{P(S_1)-1} \cdots \sum_{j_n=0}^{P(S_n)-1} \bigtriangleup_{i=1}^{n} b_{ij_i} \bigtriangleup_{i=1}^{n} b_{ij_i+\tau_i} \quad \text{...(21)}$$

τ_i represents the phase shift for the sequence S_i, where $0\le\tau_i\le P(S_i)-1$, $1\le i\le n$, notice:

$$\bigtriangleup_{i=1}^{n} b_{ij_i} \cdot \bigtriangleup_{i=1}^{n} b_{ij_i+\tau_i} = 1 - \frac{1}{2^{n-1}} \left[\prod_{i=1}^{n} (1 - b_{ij_i}) + \prod_{i=1}^{n} (1 - b_{ij_i+\tau_i}) \right] + \frac{1}{2^{2n-2}} \prod_{i=1}^{n} (1 - b_{ij_i})(1 - b_{ij_i+\tau_i}) \quad \text{...(22)}$$

Substitute equation (22) in (21) and by using equation (19) we get:

$$d_S(\tau)=\prod_{i=1}^{n}P(S_i)-\frac{1}{2^{n-1}}[\prod_{i=1}^{n}\sum_{j_i=0}^{P(S_i)-1}(1-b_{ij_i})+\prod_{i=1}^{n}\sum_{j_i=0}^{P(S_i)-1}(1-b_{ij_i+\tau_i})+\frac{1}{2^{2n-2}}\prod_{i=1}^{n}\sum_{j_i=0}^{P(S_i)-1}(1-b_{ij_i})(1-b_{ij_i+\tau_i})]$$

$$=\prod_{i=1}^{n}P(S_i)-\frac{1}{2^{n-1}}(2^{\sum_{i=1}^{n}r_i}+2^{\sum_{i=1}^{n}r_i})+\frac{1}{2^{2n-2}}\prod_{i=1}^{n}\sum_{j_i=0}^{P(S_i)-1}\left[1-(b_{ij_i}+b_{ij_i+\tau_i})+b_{ij_i}\cdot b_{ij_i+\tau_i}\right]$$

$$d_S(\tau)=\prod_{i=1}^{n}P(S_i)-2^{\sum_{i=1}^{n}r_i-n+2}+\frac{1}{2^{2n-2}}\prod_{i=1}^{n}\left[2^{r_i}+1+d_{r_i}(\tau_i)\right]$$

Because of equation (12) we have:

$$d_{r_i}(\tau_i)+1=\begin{cases}2^{r_i}, & \tau_i=0,P(S_i)\\ 0, & 0<\tau_i<P(S_i)\end{cases} \qquad \text{...(23)}$$

From equation (20) and by using equation (23) and because of Golomb 3rd theorem, two states can be concluded where $0<\tau\le P(S)-1$:

1. **if $\tau\not\equiv 0 \pmod{T_k^t}$, $\forall 1\le k\le n$, $t\in\{1,2,\ldots,C_k^t\}$, then:**

$$d_S(\tau)=P(S)-2^{\sum_{i=1}^{n}r_i-n+2}+\frac{1}{2^{2n-2}}\prod_{i=1}^{n}2^{r_i}=P(S)+2^{\sum_{i=1}^{n}r_i-2n+2}-2^{\sum_{i=1}^{n}r_i-n+2}$$

or

$$d_S(\tau)=P(S)+2^{\sum_{i=1}^{n}r_i-n+2}(\frac{1}{2^n}-1) \qquad \text{...(24)}$$

2. **if $\tau\equiv 0 \pmod{T_k^t}$,**

$$d_S(\tau)=P(S)+2^{\sum_{i=1}^{n}r_i-n+2}(\frac{1}{2^{n-k}}-1) \qquad \text{...(25)}$$

Where $1\le k\le n$.

Equation (25) can be used when $\tau\not\equiv 0 \pmod{T_k^t}$, $\forall 1\le k\le n$, by considering k=0.

Table (1) describes values of $d_S(\tau)$ when use equation (19) for n=1,2,…,6.

Table (1) values of $d_S(\tau)$ when use equation (15) for n=1,2,…,6.

k	n=2	n=3	n=4	n=5	n=6
0	$+2^{\sum r_r-2}-2^{\sum r_i}$	$+2^{\sum r_r-4}-2^{\sum r_i-1}$	$+2^{\sum r_r-6}-2^{\sum r_i-2}$	$+2^{\sum r_r-8}-2^{\sum r_i-3}$	$+2^{\sum r_r-10}-2^{\sum r_i-4}$
1	$+2^{\sum r_r-1}-2^{\sum r_i}$	$+2^{\sum r_r-3}-2^{\sum r_i-1}$	$+2^{\sum r_r-5}-2^{\sum r_i-2}$	$+2^{\sum r_r-7}-2^{\sum r_i-3}$	$+2^{\sum r_r-9}-2^{\sum r_i-4}$
2	P(S)	$+2^{\sum r_r-2}-2^{\sum r_i-1}$	$+2^{\sum r_r-4}-2^{\sum r_i-2}$	$+2^{\sum r_r-6}-2^{\sum r_i-3}$	$+2^{\sum r_r-8}-2^{\sum r_i-4}$
3	----	P(S)	$+2^{\sum r_r-3}-2^{\sum r_i-2}$	$+2^{\sum r_r-5}-2^{\sum r_i-3}$	$+2^{\sum r_r-7}-2^{\sum r_i-4}$
4	----	----	P(S)	$+2^{\sum r_r-4}-2^{\sum r_i-3}$	$+2^{\sum r_r-6}-2^{\sum r_i-4}$
5	----	----	----	P(S)	$+2^{\sum r_r-5}-2^{\sum r_i-4}$
6	----	----	----	----	P(S)

Note: in table(1), the sign + mean P(S)+

Example (1):

Let n=3, r_1=2, r_2=3, r_3=5, C_1^3=3, C_2^3=3, C_3^3=1.

$\therefore T_1^1$=3, T_1^2=7, T_1^3=31, T_2^1=21, T_2^2=93, T_2^3=217, T_3^1=651.

1. **if $\tau \not\equiv 0 (\mathrm{mod}\, T_k^t)$, $\forall 1 \le k \le 3$, then: from equation (24): $d_S(\tau)=651+2^{10-6+2}-2^{10-3+2}=203$ and $C_S(\tau)=-1/203$.**
2. **if $\tau \equiv 0 (\mathrm{mod}\, T_k^t)$, for $1 \le k \le 3$, then: by using (25):**
   a. **k=1, $d_S(\tau)=651+29(\frac{1}{2^2}-1)=267$.**
   b. **k=2, $d_S(\tau)=651+29(\frac{1}{2}-1)=395$.**
   c. **k=3, $d_S(\tau)=651$.**

Notice that frequency of $\tau \not\equiv 0 (\mathrm{mod}\, T_k^t)$ is more than other values, that because of the 1st state occurs more than the 2nd state. The 1st state occurs exactly Φ(P(S)) (Φ denotes Euler function [1]), since its represents the number of the relatively prime numbers with P(S). Actually, we know that $P(S)=\prod_{i=1}^{n} P_i=\prod_{i=1}^{n}(2^{r_i}-1)=\prod_{i=1}^{n} p_i^{q_i}$, where p_i are primes chosen as large as

possible and q_i are non-negative integers, then p_i-1 approaches p_i, that implies $\Phi(P(S))$ approaches P(S), and that what will proved in the next lemma.

Lemma (6): The proportion of $\Phi(P(S))$ to P(S) is approach 1.

Proof:

$$\frac{\Phi(P(S))}{P(S)} = \frac{\prod_{i=1}^{n} p_i^{q_i-1}(p_i-1)}{\prod_{i=1}^{n} p_i^{q_i}} = \frac{\prod_{i=1}^{n}(p_i-1)}{\prod_{i=1}^{n} p_i} \qquad \text{...(26)}$$

In equation (26) as p_i be large as possible $\Rightarrow$ p_i-1$\rightarrow p_i$.

$$\therefore \frac{\Phi(P(S)}{P(S)} \approx 1.$$

Example (2):

Table (2) shows the proportion of $\Phi(P(S))$ to P(S) for various lengths.

Table (2) the proportion of $\Phi(P(S))$ to P(S) for various lengths.

n	r_i	$P(S_i)$	P(S)	$\Phi(P(S))$	Proportion
2	2,5	3,31	93	60	65%
	3,4	7,15	105	48	46%
3	2,3,5	3,7,31	651	360	55%
	3,5,7	7,31,127	27559	22580	82%
	5,7,13	31,127,8191	32247967	3095820	96%

Brüer System (3-BKG)

Notice that:

$q_m=(b_{1m}*b_{2m})\ (b_{1m}*b_{3m})\ (b_{2m}*b_{3m})$, m=0,…,P(S)-1.

Before involved in calculating $\sum_{m=0}^{P(S)-1} q_m$ we have to prove the following facts:

Fact (1): if $a\in\{-1,1\}$, then $a^2=1$.

Proof: is trivial.

Fact (2): The distributive law of the operation (*) on (·) is satisfied s.t.

$A*(bc)=(a*b)(a*c)$, where $a,b,c\in\{-1,1\}$.

Proof:

$$(a*b)(a*c)= [1-\tfrac{1}{2}(1-a)(1-b)]\,[1-\tfrac{1}{2}(1-a)(1-c)]=1-\tfrac{1}{2}[(1-a)(1-b)+(1-a)(1-c)]$$
$$+\tfrac{1}{4}(1-a)^2(1-b)(1-c)=1-\tfrac{1}{2}[1-(a+b)+ab+1-(a+c)+ac]$$

Using fact (4.1), then:

$$(a*b)(a*c)=1-\tfrac{1}{2}[2-(2a+b+c)+ab+ac]+\tfrac{1}{4}[1-(a+b+c)+ab+ac+2bc-abc]$$
$$=1-\tfrac{1}{2}[1-(a+bc)+abc]=1-\tfrac{1}{2}(1-a)(1-bc)=a*(bc)$$

Fact (3): Let $\{a_i\}$ be maximal sequence generated from MLFSR with length r, then: $\sum_{i=0}^{P(S_r)-1} a_i * b=(2^{r-1}-1)+b\cdot 2^{r-1}$, where $a_i, b\in\{-1,1\}$.

Proof:

$$\sum_{i=0}^{P(S_r)-1} a_i * b = a_0*b+a_1*b+\ldots+a_{P(Sr)-1}b.$$

Since $a_i*b=1-\tfrac{1}{2}(1-a_i)(1-b)$ =

$$\begin{cases} 1, & \text{if } a_i=1 \\ b, & \text{if } a_i=-1 \end{cases}$$

and since $N(1)=2^{r-1}-1$ and $N(-1)=2^{r-1}$, then:

$$\sum_{i=0}^{P(r)-1} a_i * b = \underbrace{1+1+\ldots+1}_{2^{r-1}-1 \text{ times}} + \underbrace{b+b+\ldots+b}_{2^{r-1} \text{ times}} = (2^{r-1}-1)+b\cdot 2^{r-1}=2^{r-1}(1+b)-1$$

Fact (4): $\{a_i\}$ and $\{b_j\}$ are two maximal sequences generated from two MLFSR with length r_1 and r_2 respectively, then:

$$\sum_{i=0}^{P(S_1)-1}\sum_{j=0}^{P(S_2)-1} a_i * b_j = 1$$, where $a_i, b_j \in \{-1,1\}$.

Proof:

Since $\sum_{i=0}^{P(S_1)-1} a_i = -1$ and $\sum_{j=0}^{P(S_2)-1} b_j = -1$ then:

$$\sum_{i=0}^{P(S_1)-1}\sum_{j=0}^{P(S_2)-1} a_i * b_j = \sum_{i=0}^{P(S_1)-1} a_i \sum_{j=0}^{P(S_2)-1} b_j = (-1)(-1)=1$$

Fact (5): if $\{a_i\}$ maximal sequence generated from MLFSR with length r, then:

$$\sum_{i=0}^{P(r)-1} (a_i * b) \cdot a_i b = (2^{r-1}-1)b + 2^{r-1}.$$

Proof:

Since $a_i * b = \begin{cases} 1, & \text{if } a_i = 1 \\ b, & \text{if } a_i = -1 \end{cases}$, then $(a_i * b)a_i = \begin{cases} 1, & \text{if } a_i = 1 \\ -b, & \text{if } a_i = -1 \end{cases}$

$$\sum_{i=0}^{P(r)-1} (a_i * b) \cdot a_i b = b \sum_{i=0}^{P(r)-1} (a_i * b) \cdot a_i = b(2^{r-1}-1) - b2^{r-1} = (2^{r-1}-1)b - 2^{r-1}$$

(using Fact (1) and Fact(3)).

Now we are ready to calculate $\sum_{m=0}^{P(S)-1} q_m$ by using the next lemma.

Lemma (7):

$$\sum_{m=0}^{P(S)-1} q_m = -(2^{r_1+r_2-1} + 2^{r_1+r_3-1} + 2^{r_2+r_3-1}) + (2^{r_1} + 2^{r_2} + 2^{r_3}) - 1 \qquad \text{...(27)}$$

Proof:

$$\sum_{m=0}^{P(S)-1} q_m = \sum_{i=0}^{P(S_1)-1}\sum_{j=0}^{P(S_2)-1}\sum_{k=0}^{P(S_3)-1}(b_{1i} * b_{2j})(b_{1i} * b_{3k})(b_{2j} * b_{3k}) \qquad \text{...(28)}$$

$$= (2^{r_3-1}-1)\sum_{i=0}^{P(S_1)-1}\left[(2^{r_3-1}-1)+2^{r_3-1}b_{1i}\right]+2^{r_3-1}\sum_{i=0}^{P(S_1)-1}\left[(2^{r_2-1}-1)b_{1i}-2^{r_2-1}\right]$$

$$= (2^{r_3-1}-1)(2^{r_2-1}-1)(2^{r_1}-1)-(2^{r_3-1}-1)2^{r_2-1}-2^{r_3-1}(2^{r_2-1}-1)-2^{r_3-1}2^{r_2-1}(2^{r_1}-1)$$

$$\sum_{m=0}^{P(S)-1} q_m = -(2^{r_1+r_2-1}+2^{r_1+r_3-1}+2^{r_2+r_3-1})+(2^{r_1}+2^{r_2}+2^{r_3})-1$$

Equation (27) can be written as:

$$\sum_{m=0}^{P(S)-1} q_m = -\sum_{j=1}^{3} 2^{R_2^j-1}+\sum_{j=1}^{3} 2^{r_j}-1$$

Before we calculating $d_S(\tau)$ we need the following Lemmas.

Lemma (8):

$$\sum_{i=0}^{P(S_1)-1}\sum_{j=0}^{P(S_2)-1}(b_{1i} * b_{2j})(b_{1i+\tau_1}+b_{2j+\tau_2})(b_{1i}b_{2j}+b_{1i+\tau_1}b_{2j+\tau_2})$$

$$= 2-2^{r_1+r_1}-(d_{r_1}(\tau_1)+1)(d_{r_2}(\tau_2)+1)-\tfrac{1}{2}(2^{r_1}+1+d_{r_1}(\tau_1)(2^{r_2}+1+d_{r_2}(\tau_2) \qquad \text{...(29)}$$

Proof:

$$\sum_{i=0}^{P(S_1)-1}\sum_{j=0}^{P(S_2)-1}(b_{1i} * b_{2j})(b_{1i+\tau_1}+b_{2j+\tau_2})(b_{1i}b_{2j}+b_{1i+\tau_1}b_{2j+\tau_2})$$

$$= \sum_{i=0}^{P(S_1)-1} b_{1i}\sum_{j=0}^{P(S_2)-1} b_{2j}+\sum_{i=0}^{P(S_1)-1} b_{1i+\tau_1}\sum_{j=0}^{P(S_2)-1} b_{2j+\tau_2}-\tfrac{1}{2}[\sum_{i=0}^{P(S_1)-1}(1-b_{1i})b_{1i}\sum_{j=0}^{P(S_2)-1}(1-b_{2i})b_{2i}$$

$$+\sum_{i=0}^{P(S_1)-1}(1-b_{1i})b_{1i+\tau_1}\sum_{j=0}^{P(S_2)-1}(1-b_{2i})b_{2i+\tau_2}+\sum_{i=0}^{P(S_1)-1}(1-b_{1i+\tau_1})b_{1i}\sum_{j=0}^{P(S_2)-1}(1-b_{2i+\tau_2})b_{2i}$$

$$+\sum_{i=0}^{P(S_1)-1}(1-b_{1i+\tau_1})b_{1i+\tau_1}\sum_{j=0}^{P(S_2)-1}(1-b_{2i+\tau_2})b_{2i+\tau_2}]+\tfrac{1}{4}[\sum_{i=0}^{P(S_1)-1}(1-b_{1i})(1-b_{1i+\tau_1})b_{1i}\sum_{j=0}^{P(S_2)-1}(1-b_{2i})(1-b_{2i+\tau_2})b_{2i}$$

$$+\sum_{i=0}^{P(S_1)-1}(1-b_{1i})(1-b_{1i+\tau_1})b_{1i+\tau_1}\sum_{j=0}^{P(S_2)-1}(1-b_{2i})(1-b_{2i+\tau_2})b_{2i+\tau_2}]$$

$$=1+1-\tfrac{1}{2}[(P(r_1)+1)(P(r_2)+1)+(d_{r_1}(\tau_1)+1)(d_{r_2}(\tau_2)$$

$$+(d_{r_1}(\tau_1)+1)(d_{r_2}(\tau_2)+1)+(P(r_1)+1)(P(r_2)+1)]$$

$$+\tfrac{1}{4}[(P(r_1)+2+d_{r_1}(\tau_1))(P(r_2)+2+d_{r_2}(\tau_2))(P(r_1)+2+d_{r_1}(\tau_1))(P(r_2)+2+d_{r_2}(\tau_2))]$$

$$=2-2^{r_1+r_1}-(d_{r_1}(\tau_1)+1)(d_{r_2}(\tau_2)+1)-\tfrac{1}{2}(2^{r_1}+1+d_{r_1}(\tau_1)(2^{r_2}+1+d_{r_2}(\tau_2)$$

Lemma (9):

$$\sum_{i=0}^{P(S_1)-1}\sum_{j=0}^{P(S_2)-1}(b_{1i}*b_{2j})(b_{1i+\tau_1}*b_{2j+\tau_2})(b_{1i}b_{2j}b_{1i+\tau_1}b_{2j+\tau_2})$$

$$=d_{r_1}(\tau_1)d_{r_2}(\tau_2)-(d_{r_1}(\tau_1)+1)(d_{r_2}(\tau_2)+1)-\tfrac{1}{4}(2^{r_1}+1+d_{r_1}(\tau_1)(2^{r_2}+1+d_{r_2}(\tau_2) \qquad \textbf{...(30)}$$

Proof:

$$\sum_{i=0}^{P(S_1)-1}\sum_{j=0}^{P(S_2)-1}(b_{1i}*b_{2j})(b_{1i+\tau_1}*b_{2j+\tau_2})(b_{1i}b_{2j}b_{1i+\tau_1}b_{2j+\tau_2})$$

$$=\sum_{i=0}^{P(S_1)-1}\sum_{j=0}^{P(S_2)-1}\{1-\tfrac{1}{2}[(1-b_{1i})(1-b_{2j})+(1-b_{1i+\tau_1})(1-b_{2j+\tau_2})]$$

$$+\tfrac{1}{4}[(1-b_{1i})(1-b_{2j})(1-b_{1i+\tau_1})(1-b_{2j+\tau_2})]\}(b_{1i}b_{2j}b_{1i+\tau_1}b_{2j+\tau_2})$$

$$=\sum_{i=0}^{P(S_1)-1}b_{1i}b_{1i+\tau_1}\sum_{j=0}^{P(S_2)-1}b_{2j}b_{2j+\tau_2}-\tfrac{1}{2}[\sum_{i=0}^{P(S_1)-1}(1-b_{1i})b_{1i}b_{1i+\tau_1}\sum_{j=0}^{P(S_2)-1}(1-b_{2j})b_{2j}b_{2j+\tau_2}$$

$$+\sum_{i=0}^{P(S_1)-1}(1-b_{1i+\tau_1})b_{1i}b_{1i+\tau_1}\sum_{j=0}^{P(S_2)-1}(1-b_{2j+\tau_2})b_{2j}b_{2j+\tau_2}]$$

$$+\tfrac{1}{4}\sum_{i=0}^{P(S_1)-1}(1-b_{1i})(1-b_{1i+\tau_1})b_{1i}b_{1i+\tau_1}\sum_{j=0}^{P(S_2)-1}(1-b_{2j})(1-b_{2j+\tau_2})b_{2j}b_{2j+\tau_2}$$

$$= d_{r_1}(\tau_1)d_{r_2}(\tau_2) - \tfrac{1}{2}[(d_{r_1}(\tau_1)+1)(d_{r_2}(\tau_2)+1) + (d_{r_1}(\tau_1)+1)(d_{r_2}(\tau_2)+1)]$$

$$+ \tfrac{1}{4}(P(r_1)+2+d_{r_1}(\tau_1))(P(r_1)+2+d_{r_1}(\tau_1))$$

$$= d_{r_1}(\tau_1)d_{r_2}(\tau_2) - (d_{r_1}(\tau_1)+1)(d_{r_2}(\tau_2)+1) - \tfrac{1}{4}(2^{r_1}+1+d_{r_1}(\tau_1)(2^{r_2}+1+d_{r_2}(\tau_2)$$

Now we will shifting Q_m by τ to find $d_S(\tau)$ by using the next theorem.

Theorem (3):

$$\mathbf{d_S(\tau)=} \tfrac{1}{4}[d_{r_1}(\tau_1)(P(r_2)P(r_3)-2) + d_{r_2}(\tau_2)(P(r_1)P(r_3)-2) + d_{r_3}(\tau_3)(P(r_1)P(r_2)-2)$$
$$+ 2(P(r_1)+P(r_2)+P(r_3)) + d_{r_1}(\tau_1)d_{r_2}(\tau_2)d_{r_3}(\tau_3)] \qquad \textbf{...(31)}$$

Proof:

$$\mathbf{d_S(\tau)=} \sum_{m=0}^{P(S)-1} Q_m = \sum_{i=0}^{P(S_1)-1}\sum_{j=0}^{P(S_2)-1}\sum_{k=0}^{P(S_3)-1}(b_{1i} * b_{2j})(b_{1i} * b_{3k})(b_{2j} * b_{3k})$$

$$(b_{1i+\tau_1} * b_{2j+\tau_2})(b_{1i+\tau_1} * b_{3k+\tau_3})(b_{2j+\tau_2} * b_{3k+\tau_3})$$

$$= \sum_{i=0}^{P(S_1)-1}\sum_{j=0}^{P(S_2)-1}(b_{1i} * b_{2j})(b_{1i+\tau_1} * b_{2j+\tau_2}) \sum_{k=0}^{P(S_3)-1}[1-\tfrac{1}{2}(1-b_{1i}b_{2j})(1-b_{3k})][1-\tfrac{1}{2}(1-b_{1i+\tau_1}b_{2j+\tau_2})(1-b_{3k+\tau_3})]$$

$$= \sum_{i=0}^{P(S_1)-1}\sum_{j=0}^{P(S_2)-1}(b_{1i} * b_{2j})(b_{1i+\tau_1} * b_{2j+\tau_2})\{P(r_3) - 2^{r_3} + 2^{r_3-1}b_{1i}b_{2j}$$

$$+ \tfrac{1}{4}(1-b_{1i}b_{2j})(1-b_{1i+\tau_1}b_{2j+\tau_2})(2^{r_3}+1+d_{r_3}(\tau_3))\}$$

$$= 2^{r_3-1}\sum_{i=0}^{P(S_1)-1}\sum_{j=0}^{P(S_2)-1}(b_{1i} * b_{2j})(b_{1i+\tau_1} * b_{2j+\tau_2})(b_{1i}b_{2j} + b_{1i+\tau_1}b_{2j+\tau_2})$$

$$+ \tfrac{1}{4}(2^{r_3}+1+d_{r_3}(\tau_3))\{\sum_{i=0}^{P(S_1)-1}\sum_{j=0}^{P(S_2)-1}(b_{1i} * b_{2j})(b_{1i+\tau_1} * b_{2j+\tau_2})$$

$$- \sum_{i=0}^{P(S_1)-1}\sum_{j=0}^{P(S_2)-1}(b_{1i} * b_{2j})(b_{1i+\tau_1} * b_{2j+\tau_2})(b_{1i}b_{2j} + b_{1i+\tau_1}b_{2j+\tau_2})$$

$$+\sum_{i=0}^{P(S_1)-1}\sum_{j=0}^{P(S_2)-1}(b_{1i}*b_{2j})(b_{1i+\tau_1}*b_{2j+\tau_2})(b_{1i}b_{2j}b_{1i+\tau_1}b_{2j+\tau_2})\}$$ **...(32)**

By substitute equations (19), (29) and (30) in equation (32) and simplify them we get:

$$d_S(\tau)=2^{r_3-1}[2-2^{r_1+r_2}-(d_{r_1}(\tau_1)+1)(d_{r_2}(\tau_2)+1)+\tfrac{1}{2}(2^{r_1}+1+d_{r_1}(\tau_1))(2^{r_2}+1+d_{r_2}(\tau_2))]$$

$$+\tfrac{1}{4}(2^{r_3}+1+d_{r_3}(\tau_3))[P(r_1)P(r_2)-2+d_{r_1}(\tau_1)d_{r_2}(\tau_2)]$$

$$-[P(r_1)P(r_2)-2^{r_1+r_2}+\tfrac{1}{4}(2^{r_1}+1+d_{r_1}(\tau_1))(2^{r_2}+1+d_{r_2}(\tau_2))]$$

After reformulate the above equation we get:

$$d_S(\tau)=\tfrac{1}{4}[d_{r_1}(\tau_1)(P(r_2)P(r_3)-2)+d_{r_2}(\tau_2)(P(r_1)P(r_3)-2)+d_{r_3}(\tau_3)(P(r_1)P(r_2)-2)$$
$$+2(P(r_1)+P(r_2)+P(r_3))+d_{r_1}(\tau_1)d_{r_2}(\tau_2)d_{r_3}(\tau_3)]$$

equation (31) can be written in the form:

$$d_S(\tau)=\tfrac{1}{4}[d_{r_1}(\tau_1)(2^{r_2+r_3}-2^{r_2}-2^{r_3}-1)+d_{r_2}(\tau_2)(2^{r_1+r_3}-2^{r_1}-2^{r_3}-1)$$

$$+d_{r_3}(\tau_3)(2^{r_1+r_2}-2^{r_1}-2^{r_2}-1)+2(2^{r_1}+2^{r_2}+2^{r_3}-1)$$

$$+d_{r_1}(\tau_1)d_{r_2}(\tau_2)d_{r_3}(\tau_3)]-1$$ **…(33)**

According to the values of $d_{r_i}(\tau_i)$**, 1≤i≤3, there are different values to** $d_S(\tau)$**. Table (3) shows the different phases of equation (33) where** τ **divides** T_m^t **(or not), 1≤m≤3, 1≤t≤** C_m^t **.**

Table (3) Different phases of equation (33).

St	m	t	$t\mid T_m^t$	$d_{r_i}(\tau_i)$	$d_S(\tau)$
1	1	1	T_1^1=P(r_1)	$d_{r_2}(\tau_2)=d_{r_3}(\tau_3)$=-1	$2^{R_3^1-2}-(2^{R_2^1-1}+2^{R_2^2-1}+2^{R_2^3-2})+\sum_{i=1}^{3}2^{r_i}-1$
2	1	2	T_1^2=P(r_2)	$d_{r_1}(\tau_1)=d_{r_3}(\tau_3)$=-1	$2^{R_3^1-2}-(2^{R_2^1-1}+2^{R_2^2-2}+2^{R_2^3-1})+\sum_{i=1}^{3}2^{r_i}-1$
3	1	3	T_1^3=P(r_3)	$d_{r_1}(\tau_1)=d_{r_2}(\tau_2)$=-1	$2^{R_3^1-2}-(2^{R_2^1-2}+2^{R_2^2-1}+2^{R_2^3-1})+\sum_{i=1}^{3}2^{r_i}-1$
4	2	1	T_2^1=P(r_1) P(r_2)	$d_{r_3}(\tau_3)$=-1	$2^{R_3^1-1}-(2^{R_2^1}+2^{R_2^2-1}+2^{R_2^3-1})+\sum_{i=1}^{3}2^{r_i}-1$
5	2	2	T_2^2=P(r_1) P(r_3)	$d_{r_2}(\tau_2)$=-1	$2^{R_3^1-1}-(2^{R_2^1-1}+2^{R_2^2}+2^{R_2^3-1})+\sum_{i=1}^{3}2^{r_i}-1$
6	2	3	T_2^3=P(r_2) P(r_3)	$d_{r_1}(\tau_1)$=-1	$2^{R_3^1-1}-(2^{R_2^1-1}+2^{R_2^2-1}+2^{R_2^3})+\sum_{i=1}^{3}2^{r_i}-1$
7	3	1	T_3^1=P(S)	--------	$2^{R_3^1-1}-\sum_{i=1}^{3}2^{R_2^i}+\sum_{i=1}^{3}2^{r_i}-1$=P(S)
8	-	-	$t\not\mid T_m^t$	$d_{r_1}(\tau_1)=d_{r_2}(\tau_2)=d_{r_3}(\tau_3)$=-1	$-\sum_{i=1}^{3}2^{R_2^i-2}+\sum_{i=1}^{3}2^{r_i}-1$

Example(3):

Let n=3, r_1=2, r_2=3, r_3=5, then in table (4) the different values of $d_S(\tau)$ for 3-BKG are appeared.

Table (4) the different values of $d_S(\tau)$ of example (4.13).

States	1	2	3	4	5	6	7	8
$d_S(\tau)$	155	123	99	331	283	219	651	-61

5. Applying of Chi-Square Tests on Study Cases

In this section we will apply chi-square test on the results gotten from calculations of three postulates on three study cases.

Let M be the number of categories in the sequence S, c_i be the category i, $N(c_i)$ be the observed frequency of the category c_i, Pr_i the probability of occurs of the category c_i, then the expected frequency E_i of the category c_i is $E_i=P(S)\cdot Pr_i$, the T (chi-square value) can be calculated as follows [6]:

$$T=\sum_{i=1}^{K}\frac{(N(c_i)-E_i)^2}{E_i} \qquad \text{...(34)}$$

Assuming that T distributed according to chi-square distribution by υ=M-1 freedom degree by α as significance level (as usual α=0.05%), which it has T_0 as a pass mark. If $T\le T_0$ then the hypothesis accepted and the sequence pass the test, else we reject the

hypothesis and the sequence fails to pass the test, this mean that T not distributed according to chi-square distribution.

In order to test our results we have to suggest an example suitable to our three studied cases. Let n=3, r_1=7, r_2=9 and r_3=11. P(S)= 132844159, E_i=66422079.5.

In Auto correlation test υ= 1, with α=0.05%, then T_0=3.84 (see chi-square table). Since $d_S(\tau)$ represent between the $N_S(-1)$ and $N_S(1)$ for the sequence S when its shifted by τ, then its can be used to estimate the statistic value T of chi square test. We can reformulate equation (34) to be suitable to autocorrelation test, so it can written as follows:

$$T(\tau)=\frac{d_S^2(\tau)}{P(S)} \qquad \text{...(35)}$$

1. 3-PKG:

For the 3-PKG, from equation (20) and because of equation (24) then (35) will be:

$$T=\left(P(S)+2^{\sum_{i=1}^{n} r_i - n + 2}\left(\frac{1}{2^n}-1\right)\right)^2/P(S) \qquad \ldots(36)$$

When substitute the information of the chosen example in equation (36), then:

T=41247867.01 >> 3.84 then 3-PKG fail to pass this test.

2. 3-BKG:

For the 3-BKG, from equation (20) and because of equation (24) then (35) will be:

$$T=\left(-\sum_{i=1}^{3} 2^{R_2^i - 2} + \sum_{i=1}^{3} 2^{r_i} - 1\right)^2/P(S) \qquad \ldots(37)$$

When substitute the information of the chosen example in equation (37), then:

T= 877.255 > 3.84, then 3-BKG fail to pass this test. But if we choose local sequence then results of this test will passes this test. Compare this result with value of T in 3-PKG we will notice a big difference.

6. Conclusions and Future Work

1. **In this work we prove that the product cryptosystem has weak statistical autocorrelation properties deterministically, while Brüer has good statistical autocorrelation properties.**
2. **These theoretical studies can be applied on other kind of KG,s to calculate the autocorrelation of these KG,s which are use combining functions with some combinations of variables.**
3. **As future work we may apply other properties of randomness criterion like, run and autocorrelation on linear or non-linear KG.**

References

[1]. **Stallings, W., "Cryptography and Net-work Security: Principles and Practices", Pearson Prentice-Hall, 4th Edition, 2006.**

[2]. **Brüer, J. O., "On Nonlinear Combinations of Linear Shift Register Sequences", Internal Report LITH-ISY-1-0572,1983**

[3]. **Dr. Abdul Monem S. Rahma, Dr. Nadia M. G. Al-Saidi, and Ayad G. Nasser, "The Theoretic Estimation of the Basic Criterions to Evaluate the Key Generator Efficiency before the Practical Construction", The 1st Conference of Iraqi Association of Information Technology-Iraq, 17, Jen., 2009.**

[4]. **Golomb, S. W., "Shift Register Sequences" San Francisco: Holden Day 1967.**

[5]. **Brüer, J. O., "On Nonlinear Combinations of Linear Shift Register Sequences" Internal Report LITH-ISY-1-0572,1983.**

[6]. **Martinez, W. L. and Martinez, A. R., "Computational Statistics Handbook with MATLAB", Chapman & Hall/CRC, Library of Congress Cataloging-in-Publication Data, 2002.**

اجراء الحساب النظري لمقياس الارتباط الذاتي للمتتابعة المولدة من مولدات المفاتيح غير الخطية

أ.د. عبد المنعم ابو طبيخ
الجامعة التكنولوجيا

اياد غازي ناصر
الجامعة التكنولوجيا

المستخلص:

تعتبر العشوائية (Randomness) من اهم مقاييس الكفاءة الاساسية لمولدات المفاتيح (Key Generator Efficiency) المتمثل. مولد المفاتيح يعتمد بشكل اساسي على المسجل الزاحف الخطي ذو التغذية الخلفية (Linear Feedback Shift Rrgister) كونه أحد الوحدات الاساسية لنظم التشفير الانسيابي (Stream Cipher Systems). في هذا البحث، تم حساب خاصية الارتباط الذاتي، باعتبارها احد اسس العشوائية، لمتتابعة مولدة من مولد مفاتيح غير خطي نظرياً قبل تنفيذ النظام عمليا (برمجيا او مادياً)، وهذا الاسلوب سوف يوفر الوقت والجهد والكلفة لمصمم الشفرة. تم اختيار مولدي مفاتيح غير خطية لتطبيق الدراسة النظرية للبحث هما المنظومة الضربية ومولد بريور.